UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

In re: Netgain Technology, LLC, Consumer Data Breach Litigation	Case No. 21-cv-1210 (SRN/LIB) **MEMORANDUM OPINION AND ORDER**

Brian C. Gudmundson, Michael J. Laird, and Rachel K. Tack, Zimmerman Reed LLP, 1100 IDS Center, 80 South Eighth Street, Minneapolis, MN 55402; Bryan L. Bleichner, Christopher P. Renz, and Jeffrey D. Bores, Chestnut Cambronne PA, 100 Washington Avenue South, Suite 1700, Minneapolis, MN 55401; Gayle M. Blatt, Casey Gerry Schenk Francavilla Blatt & Penfield, LLP, 110 Laurel Avenue, San Diego, CA 92101; Amanda M. Williams, Daniel E. Gustafson, and David A. Goodwin, Gustafson Gluek PLLC, 120 South Sixth Street, Suite 2600, Minneapolis, MN 55402; Anne T. Regan and Nathan D. Prosser, Hellmuth & Johnson PLLC, 8050 West 78th Street, Edina, MN 55439; Karen H. Riebel, Kate M. Baxter-Kauf, and Maureen K. Berg, Lockridge Grindal Nauen PLLP, 100 Washington Avenue South, Suite 2200, Minneapolis MN 55401; Nicholas Migliaccio, Migliaccio & Rathod LLP, 412 H Street Northeast, Suite 302, Washington, DC 20002; Raina Borrelli, Turke & Strauss LLP, 613 Williamson Street, Suite 201, Madison, WI 53703; and Terence Coates, Markovits, Stock & DeMarco, LLC, 119 East Court Street, Suite 500, Cincinnati, OH 45202, for Plaintiffs.

R. Henry Pfutzenreuter, Christopher A. Young, Paul R. Smith, and Sarah D. Greening, Larkin Hoffman Daly & Lindgren Ltd., 8300 Norman Center Drive, Suite 1000, Minneapolis, MN 55437, for Defendant.

SUSAN RICHARD NELSON, United States District Judge

This matter is before the Court on the Motion to Dismiss [Doc. No. 45] filed by Defendant Netgain Technology, LLC ("Netgain"). Based on a review of the files, submissions, and proceedings herein, and for the reasons below, the Court **GRANTS** in part and **DENIES** in part the motion.

I. BACKGROUND

A. The Parties

Plaintiffs in this matter are seven individuals from California, Minnesota, Nevada, South Carolina, and Wisconsin. (Am. Compl. [Doc. No. 35] ¶¶ 15–21.) They commenced this action on behalf of themselves and a putative class that may ultimately consist of "hundreds of thousands" of individuals. (*Id.* ¶ 96.)

Netgain is a Delaware corporation with its principal place of business in Minnesota. (*Id.* ¶ 22.)

B. Factual Background

1. Netgain's Business

Netgain provides third-party information technology and cybersecurity services to businesses. (*Id.* ¶ 1, 3.) Netgain's cybersecurity model requires businesses to move their information technology to a cloud-based system, which Netgain manages externally. (*Id.* ¶ 1.) Netgain specializes in serving the healthcare and accounting industries. (*Id.* ¶¶ 1–2, 24.) As part of its service, Netgain receives access to personally identifiable information ("PII"), personal health information ("PHI"), and other sensitive data (together, "Sensitive Information"). (*Id.* ¶¶ 24, 40.) Netgain stores this data on its servers. (*Id.* ¶ 40.) Netgain's clients have included Neighborhood Healthcare, Apple Valley Medical Clinic/Allina Health, Nevada Orthopedic & Spine Center, and Sandhills Medical Center. (*Id.* ¶¶ 15–21, 46.)

2. The Data Breach

In the fall of 2020, Netgain suffered a ransomware attack ("Data Breach"). (*Id.* ¶ 39.) Unauthorized individuals ("cybercriminals") gained access to the data of at least 15 clients that was stored on Netgain's servers and then exported that data out of Netgain's system. (*Id.* ¶¶ 6, 39, 41.) This data included full names, social security numbers, dates of birth, driver's license numbers, patient cardholder numbers, patient diagnosis and treatment information, clinical notes, referral requests, laboratory reports, and vaccination and immunization information, among other things. (*Id.* ¶¶ 8, 45.) The cybercriminals also encrypted certain data. (*Id.* ¶ 43.) Upon discovering the attack, Netgain shut down certain data centers and began to rebuild the affected systems. (*See id.* ¶¶ 39, 43.)

The cybercriminals issued a ransom demand to Netgain. (*Id.* ¶ 7.) Netgain allegedly paid the ransom in exchange for assurances that the cybercriminals would delete and not disclose the stolen Sensitive Information. (*Id.*)

In early 2021, Netgain began notifying clients about the Data Breach. (*Id.* ¶ 42.) Netgain notified its clients that there was an "unauthorized access to portions of the Netgain environment," which occurred as early as September 2020. (*Id.* ¶ 43.) Netgain also identified opportunities to strengthen its security system by adding new tools, adopting new policies, and implementing "around-the-clock managed detection and response service for proactive threat monitoring." (*Id.* ¶ 49.) Netgain explained that these changes would help ensure that data security remained "top-of-mind" going forward. (*Id.*)

In turn, some of Netgain's current and former clients issued press releases and notices relating to the Data Breach. (*Id.* ¶¶ 44–45, 53.) The press releases highlighted that

"certain identifiable personal and protected health information was accessed and/or acquired from Netgain's network . . . including full names and one or more of the following: Social Security numbers, dates of birth, patient cardholder numbers, and/or treatment/diagnosis information." (*Id.* ¶ 45.) Similarly, the notices stated that the stolen data may have included the patient's name, birth date, address, social security number, bank account and routing numbers, billing and medical information, driver's license number, insurance card information, and other data. (*Id.* ¶ 53.)

3. The Alleged Harm

As a direct and proximate cause of the Data Breach, Plaintiffs allege harm. (*Id.* ¶¶ 85, 113.) Plaintiffs allege that they received notice that their Sensitive Information was stolen during the Data Breach. (*Id.* ¶¶ 86–93.) They also allege that they remain "at a present and continued risk of harm due to the exposure and potential misuses of [their] personal data by [the cybercriminals]." (*Id.* ¶¶ 87–93.) In addition, each plaintiff alleges that they have taken specific actions in response to the Data Breach, as outlined below.

a. Plaintiff Misty Meier

Ms. Meier, a California resident, brings this suit on behalf of her minor child, who is also a California resident. (*Id.* ¶ 15.) Ms. Meier and her child had provided the child's Sensitive Information to Neighborhood Healthcare. (*See id.*) On April 8, 2021, Ms. Meier received a notice from Neighborhood Healthcare informing her that her child's "Sensitive Information was exposed during Netgain's Data Breach." (*Id.*) She alleges that her child is harmed by the Data Breach because the cybercriminals "may . . . use [her child's] information to take out credit cards and car loans." (*Id.* ¶ 86.) She also alleges that the

child may not know that he has been a victim for many years because he is a minor without any credit history. (*Id.*)

b. Plaintiff Jane Doe

Ms. Doe is also a resident of California. (*Id.* ¶ 16.) She gave her Sensitive Information to Health Center Partners of Southern California. (*See id.*) She was informed on May 8, 2021, that her "Sensitive Information—stored on Netgain's systems—was stolen in the Data Breach." (*Id.* ¶ 88.) In response to that notice, she "has monitored her credit using Credit Karma." (*Id.*)

c. Plaintiff Susan Reichert

Ms. Reichert is a Wisconsin resident who gave her Sensitive Information to Apple Valley Medical Clinic. (*See id.* ¶ 17.) On March 26, 2021, she received notice from the clinic that her "Sensitive Data had been compromised by a cyberattack at Netgain." (*Id.*) Since the breach, she has "spent time reviewing her credit card and banking statements to identify any fraudulent transactions." (*Id.* ¶ 89.)

d. Plaintiff Mark Kalling

Mr. Kalling is a resident of Nevada. (*Id.* ¶ 18.) He was a patient of Nevada Orthopedic & Spine Center, which sent him notice that his "Sensitive Information was stolen during Netgain's Data Breach." (*Id.*) Since the breach, his "credit card accounts experienced suspicious activity" and he "received at least four notifications of credit card fraud." (*Id.* ¶¶ 18, 90.) He has also "spent over thirty hours mitigating the damage to his credit." (*Id.*)

e. Plaintiff Robert Smithburg

Minnesota resident, Mr. Smithburg, shared his Sensitive Information with Apple Valley Medical Clinic/Allina Health. (*See id.* ¶ 19.) In March of 2021, he received notice that Netgain's "Data Breach exposed his Sensitive Information." (*Id.*) Since the Data Breach, he has spent time "signing up for credit monitoring and reviewing his credit cards and bank statements for fraudulent transactions." (*Id.* ¶ 91.)

f. Plaintiff Thomas Lindsay

Mr. Lindsay, also a resident of Minnesota, gave his Sensitive Information to Apple Valley Medical Clinic/Allina Health as well. (*See id.* ¶ 20.) He received a letter on March 26, 2021, informing him "that his Sensitive Information was stolen." (*Id.*) In response, he "spent time contacting Apply Valley Medical Clinic about the breach." (*Id.* ¶ 92.) He further alleges that he spent time "signing up for credit monitoring" and "talking to his bank and investment companies about the breach and potential fraud." (*Id.*)

g. Plaintiff Robin Guertin

Ms. Guertin is a resident of South Carolina. (*Id.* ¶ 21.) She provided her Sensitive Information to Sandhills Medical Center. (*Id.*) On March 5, 2021, she received a letter from Sandhills Medical Center warning that "her Sensitive Information was exposed during the Netgain Data Breach." (*Id.*) In response, she has "spent time signing up for credit monitoring, reviewing her banking information to identify fraudulent charges, and changing all of her passwords." (*Id.* ¶ 93.)

C. Procedural History

1. The Original Complaints

Plaintiffs separately filed four putative class actions in Minnesota federal court. (*See* Aug. 24, 2021 Order [Doc. No. 34] at 1, 3–4.) The complaints alleged a substantially similar negligence claim against Netgain. (*Id.* at 4.) Some of the Plaintiffs also raised common law and statutory claims. (*Id.*) A little more than a month after filing their respective suits, the Plaintiffs filed a Joint Motion to Consolidate Cases [Doc. No. 16], which the Court granted. (Aug. 24, 2021 Order at 9–10.)

2. The Amended Complaint

In the consolidated action, Plaintiffs filed an Amended Complaint [Doc. No. 35]. They bring suit on behalf of themselves and the following putative class: "All natural persons residing in the United States whose data was exposed as a result of the Data Breach." (Am. Compl. ¶ 94.) They also bring suit on behalf of a California Subclass and a Minnesota Subclass. (*Id.*) Plaintiffs, the Class, and the Subclasses seek declaratory, injunctive, and monetary relief, alleging claims of negligence, negligence *per se*, and violations of the Minnesota Health Records Act, Minn. Stat. §§ 144.191–.293 ("MHRA").[1] (Am. Compl. ¶¶ 101–56.)

[1] In the Amended Complaint, Plaintiffs and the California Subclass also allege violations of the California Consumer Privacy Act and the California Unfair Competition Law. (Am. Compl. ¶¶ 122–40.) However, Plaintiffs have since withdrawn those causes of action. (Pls.' Opp'n [Doc. No. 50] at 36 n.6 ("Plaintiffs are withdrawing their Third Cause of Action for violation of the California Consumer Privacy Act and their Fourth Cause of Action for violation of California's Unfair Competition Law.").) Accordingly, as it relates to Counts III and IV, the Court denies Defendant's motion to dismiss as moot.

3. Defendant's Motion to Dismiss

Shortly after Plaintiffs filed the Amended Complaint, Netgain filed this motion to dismiss, seeking dismissal under Rules 12(b)(1) and 12(b)(6) of the Federal Rules of Civil Procedure. (Def.'s Mem. [Doc. No. 47] at 9.) Under Rule 12(b)(1), Netgain contends that Plaintiffs lack Article III standing because they have not suffered an injury in fact that is fairly traceable to Netgain's alleged conduct. (*Id.* at 10–15.) Alternatively, Netgain moves for dismissal under Rule 12(b)(6) for failure to state claims for negligence, negligence *per se*, violation of the MHRA, and declaratory and injunctive relief. (*Id.* at 15–26, 39–46.)

II. DISCUSSION

A. Lack of Standing Under Rule 12(b)(1)

1. Legal Standard

The doctrine of standing limits the court's jurisdiction to "those disputes which are appropriately resolved through the judicial process." *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992) (internal quotation marks and citation omitted). To successfully plead standing under Article III of the Constitution, a plaintiff must allege facts demonstrating the existence of an actual case or controversy by showing (1) a concrete injury in fact, (2) that is fairly traceable to the challenged action, and (3) that is likely to be redressed by the relief sought. *Id.* at 560–61. "[S]tanding is to be determined as of the commencement of the suit," and the burden of establishing standing is on the party invoking federal jurisdiction. *Id.* at 561, 570 n.5. Where, as here, the defendant challenges the existence of jurisdiction on the face of the pleadings, and not through extrinsic evidence, the reviewing court must "accept as true all factual allegations in the complaint, giving no effect to

conclusory allegations of law." *Stalley v. Catholic Health Initiatives*, 509 F.3d 517, 521 (8th Cir. 2007).

2. Analysis

Defendant contends that Plaintiffs have failed to adequately plead, in the Amended Complaint, that they suffered an injury in fact that is fairly traceable to the Data Breach. (Def.'s Mem. at 10–14.) Because Netgain only challenges injury in fact and traceability, the Court limits its analysis to those two standing elements.

a. Injury in fact

Defendant argues that Plaintiffs have not alleged a concrete, particularized injury that is actual or imminent. (*Id.* at 11.) Defendant contends that Plaintiffs have instead merely alleged a risk of future injury, which it argues does not confer standing. (*Id.* at 12–14.) The Court disagrees.

The United States Constitution requires that a plaintiff allege an injury in fact in order to have standing to proceed. *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338–39 (2016), *as revised* (May 24, 2016). To demonstrate an injury in fact, a plaintiff must show that the alleged injury is " 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.' " *In re SuperValu, Inc.*, 870 F.3d 763, 768 (8th Cir. 2017) (quoting *Spokeo*, 578 U.S. at 339)). A "particularized" injury impacts the plaintiff "in a personal and individual way." *Spokeo*, 578 U.S. at 339 (internal quotation marks and citation omitted). A "concrete" injury is one that "actually exists." *Id.* at 340. And courts have found an injury in fact based on a substantial risk of future harm. *See Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414 n.5 (2013) (collecting cases).

The requirements for standing do not change in the class action context. *See Spokeo*, 578 U.S. at 338 n.6. A putative class action can proceed as long as one named plaintiff has standing. *See Horne v. Flores*, 557 U.S. 433, 446 (2009) ("Because the superintendent clearly has standing to challenge the lower courts' decisions, we need not consider whether the Legislators also have standing to do so."); *see also Vill. of Arlington Heights v. Metro. Hous. Dev. Corp.*, 429 U.S. 252, 264 (1977) ("For we have at least one individual plaintiff who has demonstrated standing to assert these rights as his own.").

The Eighth Circuit has addressed standing in a similar context. *See SuperValu*, 870 F.3d at 768. In *SuperValu*, plaintiffs, who were customers of defendants' grocery stores, alleged that their credit and debit card information was stolen by cybercriminals by means of installing malicious software on defendants' network. *Id.* at 766. Defendants moved to dismiss the complaint for lack of standing, arguing that plaintiffs did not have an injury in fact because they did not allege that the data was stolen. *Id.* at 769. But the Eighth Circuit rejected that argument. *Id.* Noting that it must draw all inferences in the plaintiffs' favor, the court highlighted other parts of the complaint that explicitly alleged that plaintiffs "suffered theft." *Id.* The court, therefore, drew the inference that plaintiffs' card information was stolen. *Id.*

For many of the same reasons, Plaintiffs have alleged an injury in fact here. Contrary to Netgain's contention, the Court finds that Plaintiffs have sufficiently alleged that their PII and PHI was stolen. Notably, four Plaintiffs allege that their Sensitive Information "was stolen," (Am. Compl. ¶¶ 18, 20, 86, 88); two allege that it was "exposed," (*id.* ¶¶ 19, 21); and one alleges that it was "compromised," (*id.* ¶ 17.) This language, along

with Plaintiffs' allegations that Netgain paid a ransom to have the cybercriminals destroy the stolen Sensitive Information, (*id.* ¶ 7), make it easy for the Court to infer that Plaintiffs' Sensitive Information was in fact stolen.

(i) Allegations of Future Harm

Next, Netgain asserts that even if the cybercriminals stole the Sensitive Information, Plaintiffs have merely alleged that future harm *may* occur, which Netgain contends is not an injury in fact, citing *SuperValu*. But, regarding future harm, the factual allegations here are different from the facts alleged in *SuperValu*. There, despite inferring that plaintiffs' card information was stolen, the Eighth Circuit found that the theft alone did not create a substantial risk of future harm. *SuperValu*, 870 F.3d at 769–72. Central to the court's reasoning was the fact that the stolen card information did not include any PII. *Id.* at 770. And without PII, the court reasoned that "there is little to no risk that anyone will use the Card Information . . . to open unauthorized accounts in the plaintiffs' names." *Id.*

Here, it is undisputed that the stolen Sensitive Information includes PII and PHI, the absence of which was significant to the Eighth Circuit in *SuperValu*. *See* 870 F.3d at 770 ("[W]e note that the allegedly stolen Card Information does not include any personally identifying information."). This emphasis strongly suggests that substantial risk of future harm is sufficiently alleged when the stolen data includes PII.

Other circuits have held that there is a substantial risk of future harm when PII and PHI is stolen. For example, the Sixth Circuit has held that plaintiffs suffer a concrete harm when they allege a substantial risk of future harm arising from data theft. *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384, 388–89 (6th Cir. 2016) (explaining that "it

would be unreasonable to expect Plaintiffs to wait for actual misuse" where they already knew "that they have lost control of their data"). The Seventh and Ninth Circuits have reached the same conclusion. *See, e.g.*, *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693–94 (7th Cir. 2015) (finding an injury in fact where plaintiffs alleged a substantial risk of future harm due to a data breach); *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1143 (9th Cir. 2010) (finding injury in fact where plaintiffs "alleged a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data" and explaining that it would be different "if no laptop had been stolen"); *but see Reilly v. Ceridian Corp.*, 664 F.3d 38, 40, 44 (3d Cir. 2011) (finding no risk of future harm because it was unknown "whether the hacker read, copied, or understood" the information, and there was "no evidence that the intrusion was intentional or malicious" or that a "taking occurred").

This caselaw supports Plaintiffs' argument that they have adequately alleged a substantial risk of future harm in this case because their PII and PHI was stolen. *See In re 21st Century Oncology Customer Data Sec. Breach Litig.*, 380 F. Supp. 3d 1243, 1253–54 (M.D. Fla. 2019) (analyzing the circuit split and explaining that the facts weigh in favor of finding an injury in fact where stolen information "includes personally identifiable information"). Like in *Galaria*, *Remijas*, and *Krottner*, Plaintiffs PII and PHI—sensitive data that was not stolen in *SuperValu*—is in the hands of ill-intentioned criminals, and Plaintiffs with credit took concrete steps to monitor their credit in response to the Data Breach. And unlike *Reilly*, there is no dispute that the criminals intentionally stole and

sought to profit from Plaintiffs' Sensitive Information.[2] As such, the Court finds that Plaintiffs have sufficiently plead a substantial risk of future harm.

(ii) Kalling's Allegations of Present Harm

Regardless, Kalling has alleged a present injury in fact. In *SuperValu*, after analyzing future harm, the Eighth Circuit went on to determine whether plaintiffs had alleged a *present* injury. *See* 870 F.3d at 772. The court focused on one of the plaintiffs, plaintiff Holmes. *Id.* Plaintiff Holmes had alleged that "he suffered a fraudulent charge on the credit card he previously used to make a purchase at one of defendants' stores affected by the data breaches." *Id.* And the court held that this alleged misuse was sufficient to demonstrate an injury in fact. *Id.* at 773.

Like plaintiff Holmes in *SuperValu*, Kalling alleges that his PII and PHI was "stolen during the data breach." (Am. Compl. ¶¶ 8, 90.) He further alleges that, since the Data Breach, he has "received at least four notifications of credit card fraud," and that he has "spent over thirty hours mitigating the damage to his credit." (*Id.* ¶¶ 18, 90.) This misuse of Kalling's Sensitive Information is a form of identify theft, and "identify theft constitutes an actual, concrete, and particularized injury." *SuperValu*, 870 F.3d at 770 (" 'Nobody

[2] Netgain notes that in *U.S. Hotel & Resort Management, Inc. v. Onity, Inc.*, Civ. No. 13-1499 (SRN/FLN), 2014 WL 3748639 (D. Minn. July 30, 2014), this Court found that the alleged future harm did not constitute an injury in fact. But that case is clearly distinguishable. There, there was no data breach. The only alleged injury was a fear of a future unauthorized entry into a hotel room due to defendant's defective door locks. *See U.S. Hotel*, 2014 WL 3748639, at *3. Yet, as explained above, Plaintiffs' Sensitive Information is already stolen. Applying the *U.S. Hotel* analogy to this case, the criminals have already broken into the room, looked around, stolen items, and U.S. Hotel has paid a ransom in hopes that the criminals will destroy the stolen items.

doubts that identify theft, should it befall one of these plaintiffs, would constitute a concrete and particularized injury.' " (quoting *Attias v. Carefirst, Inc.*, 865 F.3d 620, 627 (D.C. Cir. 2017)). Accordingly, the Court finds that Kalling has established a present injury in fact.

Even if Kalling has alleged an injury in fact, Netgain contends that his allegations are not fairly traceable to the data breach. (Def.'s Mem. at 15.) *SuperValu* is again instructive. In *SuperValu*, the defendants also argued that plaintiff Holmes' alleged present injury was not fairly traceable to the data breach. 870 F.3d at 772–73. But the Eighth Circuit held that plaintiff Holmes had met his burden of establishing a causal link by alleging the following: "[d]efendants failed to secure customer Card Information on their network; their network was subsequently hacked; customer Card Information was stolen by the hackers; and Holmes became the victim of identity theft after the data breaches." *Id.* at 772. The court found that these allegations were sufficient to plead the "specific facts that are necessary to support a link between Holmes' fraudulent charge and the data breaches." *Id.* (internal quotation marks omitted). Because plaintiff Holmes had standing, the court held that it had jurisdiction to hear the entire case. *Id.* at 774.

In much the same way, Kalling has sufficiently alleged a causal link between his harm and the Data Breach. Specifically, he alleges that (1) Netgain failed to secure his Sensitive Information on its network, (2) Netgain suffered a cyberattack, (3) his Sensitive Information was stolen by the cybercriminals, and (4) he became a victim of four instances of identity theft after the breaches. These specific allegations, in the light of the general allegations in the Amended Complaint, sufficiently plead a causal link for the purposes of Article III standing. *See SuperValu*, 870 F.3d at 772–74 (finding present injury fairly

traceable to the data breach); *see also Brown v. Medtronic, Inc.*, 628 F.3d 451, 459 (8th Cir. 2010) (explaining that standing under Article III presents only a "threshold inquiry"); *see also Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 572 U.S. 118, 134 n.6 (2014) ("Proximate causation is not a requirement of Article III standing."). Accordingly, the Court finds that Kalling's injury in fact is fairly traceable to Netgain's Data Breach.[3]

Because Kalling has alleged that he suffered an injury in fact that is fairly traceable to Netgain's data breach that is likely to be redressed by a favorable judicial decision, Kalling has Article III standing. And because only one plaintiff needs to have standing for the suit to move forward, the Court denies Netgain's motion to dismiss under Rule 12(b)(1). *See SuperValu*, 870 F.3d at 768 ("A putative class action can proceed as long as one named plaintiff has standing.").

B. Failure to State a Claim Under Rule 12(b)(6)

1. Legal Standard

When considering a motion to dismiss under Rule 12(b)(6), the Court accepts the facts alleged in the complaint as true and views those allegations in the light most favorable to the plaintiff. *Hager v. Arkansas Dep't of Health*, 735 F.3d 1009, 1013 (8th Cir. 2013). However, the Court need not accept as true wholly conclusory allegations or legal conclusions couched as factual allegations. *Id.* In addition, the Court ordinarily does not consider matters outside the pleadings on a motion to dismiss. *See* Fed. R. Civ. P. 12(d).

---

[3] Although Netgain does not challenge the final element of standing, the Court finds that Kalling's injury is likely to be redressed by a favorable judicial decision. *See Lujan*, 504 U.S. at 561.

Matters outside the pleadings include "any written or oral evidence in support of or in opposition to the pleading that provides some substantiation for and does not merely reiterate what is said in the pleadings," as well as statements of counsel at oral argument that raise new facts not alleged in the pleadings. *Hamm v. Rhone-Poulenc Rorer Pharm., Inc.*, 187 F.3d 941, 948 (8th Cir. 1999) (internal quotation marks and citation omitted). The Court may, however, "consider the pleadings themselves, materials embraced by the pleadings, exhibits attached to the pleadings, and matters of public record." *Illig v. Union Elec. Co.*, 652 F.3d 971, 976 (8th Cir. 2011) (internal quotation marks and citation omitted).

To survive a motion to dismiss, a complaint must contain "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). Although a complaint need not contain "detailed factual allegations," it must allege facts with enough specificity "to raise a right to relief above the speculative level." *Id.* at 555. "Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements," are insufficient. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citing *Twombly*, 550 U.S. at 555).

2. Analysis

The United States Supreme Court "has held an individualized choice-of-law analysis must be applied to each plaintiff's claim in a class action." *In re St. Jude Med., Inc.*, 425 F.3d 1116, 1120 (8th Cir. 2005). But courts generally decline to conduct a choice-of-law analysis prior to discovery. *See, e.g.*, *Cantonis v. Stryker Corp.*, Civ. No. 09-3509 (JRT/JJK), 2011 WL 1084971, at *3 (D. Minn. Mar. 21, 2011) (explaining that "it would

be inappropriate to engage in an analysis of what state's laws are to be used throughout the remainder of the litigation"); *Ridings v. Stryker Sales Corp.*, Civ. No. 10-2590 (MJD/FLN), 2010 WL 4963064, at *2 (D. Minn. Dec. 1, 2010) ("[A]t this point, before discovery has occurred, the Court does not have sufficient information to determine which state's law applies.").

Here, the Court finds that applying a choice-of-law analysis at this time is premature. As such, the Court analyzes Plaintiffs' state law claims of negligence and negligence *per se* under California, Minnesota, Nevada, South Carolina, and Wisconsin laws. The Court also analyzes the MHRA claim and Plaintiffs' request for declaratory and injunctive relief.

a. Negligence

A negligence claim requires a plaintiff to allege a duty, breach, causation, and injury.[4] *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1170 (D. Minn. 2014) (citing *Schmanski v. Church of St. Casimir of Wells*, 67 N.W.2d 644, 646 (Minn. 1954). Netgain argues that the negligence claim fails for three reasons. (Def.'s Mem. at 16–24.) First, the economic loss doctrine bars it. (*Id.* at 17–20.) Second, Plaintiffs have

[4] These elements of a claim for negligence are substantially identical in every jurisdiction in which Plaintiffs raise the claim. *See, e.g.*, *Hayes v. Cnty. of San Diego*, 305 P.3d 252, 255 (Cal. 2013) (California law); *Hoida, Inc. v. M & I Midstate Bank*, 717 N.W.2d 17, 27 (Wis. 2006) (Wisconsin law); *Foster v. Costco Wholesale Corp.*, 291 P.3d 150, 153 (Nev. 2012) (Nevada law); *J.T. Baggerly v. CSX Transp., Inc.*, 635 S.E.2d 97, 101 (S.C. 2006) (South Carolina law).

failed to sufficiently plead a duty. (*Id.* at 20–22.) Third, Plaintiffs' damages are speculative. (*Id.* at 22–24.) Each argument is considered in turn.

(i) Economic Loss Doctrine

Netgain contends that the economic loss doctrine bars Plaintiffs' negligence claim. (*Id.* at 17–20.) Because it is a judicially developed doctrine, *see, e.g.*, *Sheen v. Wells Fargo Bank, N.A.*, 505 P.3d 625, 627–28 (Cal. 2022), it applies differently in the various states, as discussed below.

a. Minnesota and Wisconsin

In Minnesota and Wisconsin, the economic loss doctrine does not apply to the sale of services. *Ins. Co. of N. Am. v. Cease Elec. Inc.*, 688 N.W.2d 462, 472 (Wis. 2004) ("[W]e determine that the economic loss doctrine is inapplicable to claims for the negligent provision of services."); *McCarthy Well Co., Inc. v. St. Peter Creamery, Inc.*, 410 N.W.2d 312, 315 (Minn. 1987) (holding that the economic loss doctrine only applies when a transaction is governed by the Uniform Commercial Code). Here, it is undisputed that Netgain provided cybersecurity and cloud-computing "services" to its clients. (Am. Compl. ¶¶ 1, 4, 22, 23.) Accordingly, the economic loss doctrine does not bar Plaintiffs' negligence action in Minnesota and Wisconsin.

b. South Carolina

The Supreme Court of South Carolina has held that the economic loss doctrine applies "where duties are created *solely* by contract." *Kennedy v. Columbia Lumber & Mfg. Co., Inc.*, 384 S.E.2d 730, 737 (S.C. 1989) (emphasis in original); *see also Tommy L. Griffin Plumbing & Heating Co. v. Jordan, Jones & Goulding, Inc.*, 463 S.E.2d 85, 88

(S.C. 1995) (confirming that the economic loss doctrine only applies to duties created *solely* by contract). Here, it is undisputed that Plaintiffs do not have privity of contract with Netgain, meaning no duties between the parties arise from a contract. Therefore, this negligence claim is not barred by the economic loss doctrine in South Carolina.

c. California and Nevada

The courts of California and Nevada have not addressed whether the economic loss doctrine applies in this context. Accordingly, the Court endeavors to determine whether they would apply that doctrine to the facts presented in this case.

In California and Nevada, a plaintiff may not recover in tort for purely economic damages. *See NuCal Foods, Inc. v. Quality Egg LLC*, 918 F. Supp. 2d 1023, 1028 (E.D. Cal. 2013) ("[P]urely economic losses are not recoverable in tort."); *Terracon Consultants W., Inc. v. Mandalay Resort Grp.*, 206 P.3d 81, 86 (Nev. 2009) (explaining that the economic loss doctrine generally prohibits unintentional tort actions in which the plaintiff seeks to recover purely economic losses). In Nevada, purely economic loss means "the loss of the benefit of the user's bargain . . . including . . . pecuniary damage for inadequate value, the cost of repair and replacement of the defective product, or consequent loss of profits, without any claim of personal injury or damage to other property." *Calloway v. City of Reno*, 993 P.2d 1259, 1263 (Nev. 2000) (internal quotation marks omitted) (superseded by statute on other grounds as stated in *Olson v. Richard*, 89 P.3d 31 (Nev. 2004)). California courts similarly interpret the economic loss doctrine. *See, e.g.*, *In re Ambry Genetics Data Breach Litig.*, No. SACV 20-00791-CJC (KESx), 2021 WL 4891610, at *4 (C.D. Cal. Oct. 18, 2021) (finding that purely economic losses do not

include alleged injuries of privacy, anxiety, concern, unease, and loss of time due to a data breach); *In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.*, No. 3:19-cv-2284-H-KSC, 2020 WL 2214152, at *4 (S.D. Cal. May 7, 2020) (finding same as to alleged damages of loss of time and increased anxiety due to a data breach.); *see also Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1039 (N.D. Cal. 2019) ("[P]laintiff alleged his loss of time as a harm and so does not allege pure economic loss.").

Here, the Court concludes that Plaintiffs have alleged damages that are not purely economic losses under the laws of Nevada and California. Specifically, Plaintiffs allege that the Data Breach has made the "Class's identities less secure and reliable" and that they "will also have to protect against identity theft for years to come." (Am. Compl. ¶ 113.) Like in *Ambry*, *Solara*, and *Bass*, Plaintiffs have alleged loss of time damages. These allegations go beyond purely economic loss. *See, e.g.*, *Calloway*, 993 P.2d at 1263.

Moreover, finding an exception to the economic loss doctrine in this case supports Nevada's public policy to impose liability where "the law would not exert significant financial pressures to avoid such negligence." *Terracon Consultants*, 206 P.3d at 88 (explaining why negligent misrepresentation claims are exceptions to the economic loss doctrine under Nevada law). Without tort liability in these types of cases, the law would not exert sufficient financial pressure on cybersecurity providers to properly update their systems to protect this highly sensitive information. Put another way, Netgain and its clients could negotiate limited liability in these situations, which would undermine the personal stake of those individuals whose information is at risk.

For these reasons, the Court finds that the economic loss doctrine does not bar Plaintiffs' negligence claim in Nevada and California.

(ii) Duty

Next, Netgain argues that it has no duty to protect Plaintiffs from the criminal actions of third parties. (Def.'s Mem. at 20–22.) The Court considers this argument under the law of each state.

a. California

Plaintiffs have sufficiently alleged a common law duty under California law. California courts have held that certain businesses have a duty to reasonably protect personal data. *See Castillo v. Seagate Tech., LLC*, Case No. 16-cv-01958-RS, 2016 WL 9280242, at *3 (N.D. Cal. Sept. 14, 2016) (concluding that employer had a duty to protect the personal identifying information of its employees and their spouses and dependents); *Corona v. Sony Pictures Ent., Inc.*, No. 14-CV-09600 RGK (Ex), 2015 WL 3916744, at *5 (C.D. Cal. June 15, 2015) (denying motion to dismiss the negligence claim regarding the employer's alleged duty to "maintain adequate security measures" to safeguard plaintiffs' personal information); *see also In re Facebook, Inc., Consumer Privacy User Profile Litigation*, 402 F.Supp.3d 767, 799 (N.D. Cal. 2019) (finding that plaintiffs had plausibly alleged a duty because "Facebook had a responsibility to handle its users' sensitive information with care").

Rather than allege that there is no common law duty, Netgain asserts that it has no duty to protect Plaintiffs from the intervening acts of criminals because Plaintiffs have failed to allege the existence of a "special relationship." (Def.'s Mem. at 21.) Netgain

offers no legal support, however, for its argument that no "special relationship" exists in these circumstances.

In *Castillo*, a California district court found that an employer had a duty to protect the personal information it possessed regarding the spouses and dependents of its employees and former employees, despite no privity of contract with those persons. *See* 2016 WL 9280242, at *3. In reaching this conclusion, the court considered the following factors:

> (1) the foreseeability of the harm to the plaintiff; (2) the degree of certainty that the plaintiff suffered injury; (3) the closeness of the connection between the defendant's conduct and the injury suffered; (4) the moral blame attached to the defendant's conduct; (5) the policy of preventing future harm; and (6) the extent of the burden to the defendant and consequences to the community of imposing a duty to exercise care with resulting liability for breach and the availability, cost, and prevalence of insurance for the risk involved.

Id. at *3.

Applied here, these factors suggest that Netgain owed Plaintiffs a duty to safeguard their PII and PHI. The Sensitive Information was valuable, as evidenced by Netgain's ransom payment. Further, Plaintiffs have alleged certain injury from the Data Breach, including time spent monitoring their credit reports and less secure and reliable identities. (Am. Compl. ¶¶ 85–93, 113.) Likewise, Kalling has alleged that he "received at least four notifications of credit card fraud" and "spent over thirty hours mitigating the damage." (*Id.* ¶¶ 18, 90.) And it is foreseeable that these alleged harms would result when a cybersecurity provider fails to properly protect data from its clients in the healthcare and accounting industries. To be sure, the chance that Plaintiffs may actually suffer identity theft is

unknown at this time. But it is reasonable to infer that persons whose information was stolen by cybercriminals would, at the very least, spend time and effort to detect or prevent identity theft. Additionally, imposing a common law duty on cybersecurity companies that are trusted with sensitive PII and PHI further promotes a policy of preventing identity theft and protecting the confidentiality of medical information.

These considerations were affirmed in *Bass*. There, the Northern District of California held that plaintiffs had plausibly alleged that Facebook owed them a duty. *Bass*, 394 F. Supp. 3d at 2039. In finding a duty, the court reasoned that Facebook should have known that a "lack of reasonable care in the handling of personal information can foreseeably harm the individuals providing the information," and that this was significant because some of the information was private and plaintiffs were trusting Facebook to use appropriate data security. *Id.* Notably, the court emphasized that finding no duty of care would "create perverse incentives for businesses who profit off the use of consumers' personal data to turn a blind eye and ignore known security risks." *Id.* (internal quotation marks and citation omitted).

So too here. Netgain provides cybersecurity services to its clients and Netgain should know that a lack of reasonable care creates foreseeable harm to the individuals providing that information to Netgain's clients. Like in *Bass*, this information included private information (i.e., PII and PHI) and Netgain's clients were trusting Netgain to employ appropriate data security. Accordingly, under California law, Plaintiffs plausibly plead a duty.

b. Minnesota

Under Minnesota law, an individual has a duty " 'to act with reasonable care for the protection of others' in two situations." *In re Target Corp.*, 64 F. Supp. 3d at 1308 (quoting *Domagala v. Rolland*, 805 N.W.2d 14, 23 (Minn. 1936)). First, general negligence law "imposes a general duty of reasonable care when the defendant's own conduct creates a foreseeable risk of injury to a foreseeable plaintiff." *Id.* Second, a duty arises when there is a special relationship between the defendant and the plaintiff and an "action by someone other than the defendant creates a foreseeable risk of harm to the plaintiff." *Id.*

Defendant argues that it has no duty because Plaintiffs do not adequately plead that there is a special relationship under Minnesota law. (Def.'s Mem. at 21.) But Plaintiffs contend that this is not a special relationship case, but rather a general negligence case where Netgain's own conduct, in failing to maintain appropriate data security measures, created a foreseeable risk of the harm that occurred, and Plaintiffs were the foreseeable victims of that harm. (Pls.' Opp'n at 24–29.) The Court agrees with Plaintiffs.

Minnesota courts have considered the following factors when determining whether a defendant owed a duty of care in a general negligence case: "(1) the foreseeability of harm to the plaintiff, (2) the connection between the defendant's conduct and the injury suffered, (3) the moral blame attached to the defendant's conduct, (4) the policy of preventing future harm, and (5) the burden to the defendant and community of imposing a duty to exercise care with resulting liability for breach." *In re Target Corp.*, 64 F. Supp. 3d at 1309 (citing *Domagala,* 805 N.W.2d at 26.) "The duty to exercise reasonable care arises from the probability or foreseeability of injury to the plaintiff." *Id.* And, although

usually an issue for the jury, "the foreseeability of harm can be decided by the court as a matter of law when the issue is clear." *Foss v. Kincade*, 766 N.W.2d 317, 322–23 (Minn. 2009). The Court must review these factors in the light most favorable to Plaintiffs, keeping in mind that this motion tests only the sufficiency of the pleadings and not the ultimate success of Plaintiffs' legal theories.

At this preliminary stage of the litigation, Plaintiffs plausibly plead a general negligence case. Plaintiffs sufficiently allege that Netgain's actions and inactions—implementing knowingly deficient data security measures and failing to follow its own advice for protecting against cybercriminals—caused foreseeable harm to Plaintiffs. Plaintiffs also plausibly allege that Netgain's conduct caused the harm they suffered. And Plaintiffs' allegation that Netgain was responsible to safeguard the data is also plausible. Although the third-party cybercriminals caused the harm, Netgain played a central role in permitting that harm to occur. Simply put, Plaintiffs allege that Netgain's "own conduct create[d] a foreseeable risk of injury to a foreseeable plaintiff," *Domagala*, 805 N.W.2d at 23. Accordingly, the Court finds that Plaintiffs plausibly plead a duty under Minnesota law.

c. Nevada

In Nevada, "no duty is owed to control the dangerous conduct of another." *Sanchez ex re. Sanchez v. Wal–Mart Stores, Inc.*, 221 P.3d 1276, 1280 (Nev. 2009). However, there are exceptions to that general rule, including "when (1) a special relationship exists between the parties or between the defendant and the identifiable victim, and (2) the harm created by the defendant's conduct is foreseeable." *Id.* at 1280–81. A crucial factor in

establishing liability under this exception is "the element of control." *Scialabba v. Brandise Constr. Co.*, 921 P.2d 928, 930 (Nev. 1996). In *Scialabba,* the Nevada Supreme Court held that a special relationship arose between a construction company performing work on an apartment complex and one of the tenants. *Id.* at 932. The court explained that "a duty should be imposed upon the one possessing control (and thus the power to act) to take reasonable precautions to protect the other one from assaults by third parties which, at least, could reasonably have been anticipated." *Id.* (alteration in original) (internal quotation omitted). And the court found that "the alleged failure to lock the doors to the vacant apartments created a foreseeable risk of criminal activity and harm to [the tenant]." *Id.*

The same reasoning applies here. Netgain, a third party, took exclusive control over Plaintiffs' Sensitive Information in a way that deprives them of the ability to protect that information, and where it is reasonably anticipated that cybercriminals may try to steal the information. Notably, Netgain has not cited any caselaw establishing that such a special relationship cannot arise under Nevada law. Accordingly, the Court finds that Plaintiffs plausibly plead a claim for negligence under Nevada law.

d. South Carolina

Under South Carolina law, "[a]n affirmative legal duty exists only if created by statute, contract, relationship, status, property interest, or some other special circumstance." *Hendricks v. Clemson Univ.*, 578 S.E.2d 711, 714 (S.C. 2003). In general, there is no common law duty to act; however, where an act is voluntarily undertaken, the actor assumes the duty to use due care. *Id.*; *Vaughan v. Town of Lyman*, 635 S.E.2d 631,

637 (S.C. 2006). Whether such a duty exists depends on "the relationship between the parties," and "not the potential 'foreseeability of injury.' " *Williams v. Preiss-Wal Pat III, LLC*, 17 F. Supp. 3d 528, 535 (D.S.C. 2014).

In *Shaw v. Psychemedics Corporation*, the South Carolina Supreme Court held that a duty arose from the special circumstances surrounding the contractual relationship between an employer and a drug-testing laboratory. 826 S.E.2d 281, 283 (S.C. 2019). Specifically, the court held that there was a duty of care owed by the laboratory to the employer's employees who were subject to testing at the laboratory. *Id.* In reaching this decision, the court explained that "[t]he principal purpose of the contract between the laboratory and the employer is to test a given employee's biological specimen for the presence of drugs." *Id.* at 283. The court further explained that, at some point during the testing process, if not for the entire duration, the laboratory "possesses and exercises control over the employee's specimen." *Id.* As such, the court explained that "if the laboratory is negligent in testing the employee's specimen, it is foreseeable that the employee will likely suffer a direct economic injury." *Id.* The court also highlighted that South Carolina's public policy favors recognition of a duty because (1) there is a public interest in accurate drug testing, (2) significant consequences follow from a positive drug test, and (3) the injured employee would be left without redress. *Id.* at 183–84. Therefore, the court held that there was a duty. *Id.* at 283.

The Court finds this reasoning persuasive and therefore finds that a special circumstance arose under South Carolina law in this case. Like in *Shaw*, the contractual relationship between Netgain and its clients created a special circumstance where Netgain

possessed and exercised exclusive control over Plaintiffs' Sensitive Information. If Netgain acted negligently, then Plaintiffs would suffer injury. And absent a duty, Plaintiffs effectively have no other recourse.

At least one other federal court has reached the same conclusion when applying South Carolina law. *See In re Blackbaud, Inc., Customer Data Breach Litig.*, No. 3:20-mn-02972-JMC, 2021 WL 4866393 (D.S.C. Oct. 19, 2021). In *Blackbaud*, the District of South Carolina concluded that the plaintiffs sufficiently plead an exception to the general rule that there is not duty to act. *Id.* at *7. The court held that plaintiffs had established that a third-party software and cybersecurity provider had a common law duty to maintain and secure plaintiffs' private information. *Id.* In reaching this decision, the court rejected defendant's argument that it had no duty to protect a third party from danger. *Id.* at *7–8. Instead, the court relied on South Carolina precedent that provides, as outlined above, that a duty to a third party can arise where an act is voluntarily undertaken, including through a contractual relationship. *Id.*

For these reasons, the Court finds that Plaintiffs plausibly plead a duty under South Carolina law.

e. Wisconsin

Wisconsin law provides that a duty of care is established "when it can be said that it was foreseeable that his act or omission to act may cause harm to someone." *Rockweit by Donohue v. Senecal*, 541 N.W.2d 742, 747 (Wis. 1995) (internal quotation marks and citation omitted). At a minimum, "every person is subject to a duty to exercise ordinary care in all of his or her activities." *Gritzner v. Michael R.*, 611 N.W.2d 906, 912 (Wis.

2000). The Wisconsin Supreme Court routinely employs the analysis of Restatement (Second) of Torts § 324A when determining whether such a duty arises. *Id.* at 920 ("This court has adopted the theory of negligence set forth in the Restatement (Second) of Torts § 324A."). Section 324A provides as follows:

> One who undertakes, gratuitously or for consideration, to render services to another which he should recognize as necessary for the protection of a third person or his things, is subject to liability to the third person for physical harm resulting from his failure to exercise reasonable care to protect his undertaking, if
>
> > (a) his failure to exercise reasonable care increases the risk of such harm, or
> >
> > (b) he has undertaken to perform a duty owed by the other to the third person, or
> >
> > (c) the harm is suffered because of reliance of the other or the third person upon the undertaking.

Stephenson v. Universal Metrics, Inc., 641 N.W.2d 158, 163–64 (Wis. 2002) (quoting Restatement (Second) of Torts § 324A). In *Stephenson*, the Wisconsin Supreme Court applied this standard to hold that an individual had a duty to protect a third party when he gratuitously agreed to give the third party a ride home. *Id.* at 164. The court concluded that the individual, without any duty to act, voluntarily chose to act and thus created a duty to act without negligence. *Id.* And the court concluded that "a reasonable jury could have found that [the individual] failed to exercise reasonable care, and that such a failure increased the risk of harm to other persons and property." *Id.*

In the same way, Netgain had no duty to provide cybersecurity services to businesses. However, it voluntarily reached out to potential clients as a "cybersecurity expert" and entered into agreements with them to secure PII and PHI. (Am. Compl. ¶¶ 2–

5, 23–34, 46, 81.) Like the individual in *Stephenson*, Netgain assumed this duty and thus assumed a duty not to act negligently. Moreover, it was foreseeable that cybercriminals may try to steal this information, causing harm to Plaintiffs. And Netgain knew this because its business model is premised on protecting such data from cybercriminals. Accordingly, the Court finds that Plaintiffs plausibly plead a duty under Wisconsin law.

(iii) Damages

Netgain asserts that Plaintiffs do not plead cognizable damages. (Def.'s Mem. at 22–24.) Specifically, Netgain contends that Plaintiffs' damages are speculative because they have only alleged a 25% risk that their Sensitive Information will result in identity theft. (*Id.* at 23.) The Court is unpersuaded.

Courts have held that damages like monitoring and lost time are cognizable. *See Gardner v. Health Net, Inc.*, Civ. No. 10-2140 PA (CWx), 2010 WL 11571242, at *3 (C.D. Cal. Nov. 29, 2010) (finding "credit monitoring costs" cognizable damages for a negligence claim); c*f. Potter v. Firestone Tire & Rubber Co.*, 863 P.2d 795, 824 (Cal. 1993) ("[W]e hold that the cost of medical monitoring is a compensable item of damages . . . ."); *Burlison v. Janssen*, 141 N.W.2d 274, 279 (Wis. 1966) ("A plaintiff may recover damages for lost wages or lost time . . ."); *Sieg v. Wagner*, 217 N.W. 439, 441 (Minn. 1928) (affirming "lost time" damages award in a negligence action); *Sadler v. PacifiCare of Nev.*, 340 P.3d 1264, 1270 (Nev. 2014) (discussing damages for a "medical monitoring claim").

The Court finds that Plaintiffs have alleged cognizable damages. Specifically, the Plaintiffs allege that cybercriminals stole their Sensitive Information, including full names, birth dates, social security numbers, driver's license numbers, medical records, and other

types of information. (*E.g.*, Am. Compl. ¶ 8, 53.) As a result of the breach, Plaintiffs allege damages due to Netgain's untimely and inadequate notification of the Data Breach, along with opportunity costs, loss of time costs, and out-of-pocket expenses. (*Id.* ¶ 85.) And Plaintiffs Doe, Reichert, Smithburg, Lindsay, and Guertin allege that they spent time signing up for credit monitoring. Similarly, Kalling has "received at least four notifications of credit card fraud" and "spent over thirty hours mitigating the damage." At this stage of the proceedings, this is enough for the Plaintiffs to establish cognizable damages. *See, e.g.*, *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 494 (D. Md. 2020) (rejecting argument that plaintiffs had failed to plead damages by explaining that plaintiffs "do not need to assign a value at this stage to adequately plead damages" and thus denying the motion to dismiss); *In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1317 (N.D. Ga. 2019) ("[T]he Plaintiffs here have sufficiently alleged a substantial and imminent risk of impending identity fraud due to the vast amount of information that was obtained in the Data Breach.").

The cases relied upon by Netgain are distinguishable. For example, Netgain cites a series of cases that analyze whether there was enough *evidence* introduced at trial to support a damages award. *See Holt v. Brown*, 185 F. Supp. 3d 727, 730, 739 (D.S.C. 2016) (finding, after a bench trial, that plaintiff had not established that future medical treatment was reasonably necessary); *Watt v. Nevada Cent. R. Co.*, 44 P. 423, 424, 428–29 (Nev. 1896), *modified*, 46 P. 52 (Nev. 1896) (reversing, after a bench trial, the district court's award of damages as speculative); *Johnson v. Rouchleau-Ray Iron Land Co.*, 168 N.W. 1, 2 (Minn. 1918) (holding, after trial, that apprehension of a future mud slide did not

constitute damage to real property and thus reversing district court's award of damages); *Brantner v. Jenson*, 360 N.W.2d 529, 532 (Wis. 1985) (affirming, after a jury trial, damages award because the evidence supported a finding that plaintiff's pain necessitated future surgery).

And Netgain's other citations involve circumstances where it is unknown whether the data was actually accessed by the criminals. *See Forbes v. Wells Fargo Bank, N.A.*, 420 F. Supp. 2d 1018, 1019–20 (D. Minn. 2006) (granting summary judgment because the evidence failed to show that "the information on the stolen computers has been accessed or misused"); *Gardner*, 2010 WL 11571242, at *2 (dismissing negligence claim as to plaintiff who failed to allege that her confidential information "was actually exposed"); *Rhoades v. Lourey*, No. A18-1120, 2019 WL 1006804, at *4 (Minn. Ct. App. Mar. 4, 2019) (affirming district court's determination that plaintiff failed to sufficiently plead statutory damages in part because the allegedly negligently handled private information "never left the MSOP system.").

Gardner makes this distinction plain. There, the court distinguished between one plaintiff who had *not* alleged that her data "was actually exposed," and a different plaintiff who had alleged that her information "was significantly exposed." *Gardner*, 2010 WL 11571241, at *1–3. The court dismissed the plaintiff's claim who failed to allege exposure, while permitting the other plaintiff's negligence claim to advance. *Id.* at *2–3. The court noted that the second plaintiff properly alleged that her risk of identify fraud was

"significantly increased . . . *as a result* of the exposure of [her] information." *Id.* at *3 (emphasis added).[5]

Here, as explained above, there is no dispute that the Plaintiffs' Sensitive Information was stolen and exposed. In fact, the parties agree that Netgain paid the cybercriminals an undisclosed amount of money in the hopes that the cybercriminals would destroy the Sensitive Information. Accordingly, the Court denies Netgain's motion to dismiss Plaintiffs' negligence claim.

b. Negligence *per se*

Netgain argues that Plaintiffs' claim for negligence *per se* fails because there is no private right of action under Section 5 of the Federal Trade Commission ("FTC") Act, 15 U.S.C. §§ 41-58. (Def.'s Mem. at 24–26.) The Court agrees.

A claim for negligence *per se* arises when a duty is created by statute. *E.g.*, *Sanchez*, 221 P.3d at 1283. For negligence *per se* to apply, the injured person must show that he or she is a member of the "class of persons whom the statute is intended to protect and the injury is of the type against which the statue is intended to protect." *Id.*; *Anderson v. State, Dep't of Nat. Res.*, 693 N.W.2d 181, 190 (Minn. 2005); *Hoff v. Vacaville Unified Sch. Dist.*,

[5] Netgain also cites *Pruchnicki v. Envision Healthcare Corporation*, 439 F. Supp. 3d 1226 (D. Nev. 2020), *aff'd*, 845 F. App'x 613 (9th Cir. 2021), for the proposition that lost time damages are not cognizable damages. (Def.'s Reply at 15.) However, the only Plaintiff from Nevada is Kalling, and he alleges much more than lost time damages. (Am. Compl. ¶¶ 18, 90 (alleging that he "received at least four notifications of credit card fraud" and "spent over thirty hours mitigating the damage to his credit").) Accordingly, *Pruchnicki* does not compel dismissal here.

968 P.2d 522, 530 (Cal. 1998); *Whitlaw v. Kroger Co.*, 410 S.E.2d 251, 252 (S.C. 1991); *Antwaun A. ex rel. Muwonge v. Heritage Mut. Ins. Co.*, 596 N.W.2d 456, 466 (Wis. 1999).

Here, Plaintiffs generally allege that "Plaintiffs and the Class are within the class of persons Section 5 of the FTCA (and similar state statutes) were intended to protect." (Am. Compl. ¶ 120.) This conclusory allegation fails to explain how Plaintiffs constitute members of the group that the statute was designed to protect. *See, e.g.*, *In re Blackbaud*, 2021 WL 4866393, at *11 (applying South Carolina law to dismiss plaintiffs' negligence *per se* claim for violation of the FTC Act because plaintiffs "d[id] not actually define or otherwise explain" how they were members of the group the statute was designed to protect); *Williams ex rel. Estate of Williams v. CSX Transp., Inc.*, No. 2007-MO-001, 2007 WL 8434527, at *2 (S.C. Jan. 2, 2007) (concluding that the district court erred in charging jury in negligence *per se* when it was clear that plaintiff "was not a member of the class of persons intended to be protected by [the statute]."); *Grozdanich v. Leisure Hills Health Ctr., Inc.*, 25 F. Supp. 2d 953, 986 (D. Minn. 1998) (dismissing negligence *per se* claim because "[t]he Plaintiff is simply not a member of the class of persons who were intended to be protected by the [statute]"); *Ashwood v. Clark Cnty.*, 930 P.2d 740, 744 (Nev. 1997) (affirming summary judgment on negligence *per se* claim because "as a matter of law," plaintiff was "not a member of the class of persons the [statute] . . . was meant to protect"); *Hoff*, 968 P.2d at 530 (affirming district court's grant of motion for nonsuit on negligence claim in part because the statute was not designed "to protect against the risk of injury to members of the general public").

What is more, Plaintiffs have not established that negligence *per se* can be based on a violation of Section 5 of the FTC Act. Pursuant to the FTC Act, the Federal Trade Commission has the authority to, among other things, enforce against "unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45(a). Under this authority, the Commission brings many enforcement actions "against companies that have purportedly failed to protect consumer financial data against hackers." *SuperValu*, 925 F.3d at 963. However, the FTC Act creates no private right of action. *FTC v. Johnson*, 800 F.3d 448, 452 (8th Cir. 2015).

Here, Plaintiffs have not cited any precedent in California, Minnesota, Nevada, South Carolina, or Wisconsin that permits a state-law negligence *per se* claim to proceed based on the theory that there is a violation of Section 5 of the FTC Act. Contrary to Plaintiffs' position, the Court has found one federal case applying California law, which found that a negligence *per se* claim was barred "because the FTC Act creates no private right of action." *Pica v. Delta Air Lines, Inc.*, No. CV 18-2876-MWF (Ex), 2018 WL 5861362, at *9 (C.D. Cal. Sept. 18, 2018).

The Court finds this reasoning persuasive. Simply put, the FTC Act grants the FTC enforcement authority and establishes a certain standard of care, not a private right of action. For these reasons, the Court grants Defendant's motion to dismiss Count II.

c. Minnesota Health Records Act ("MHRA")

Netgain contends that Plaintiff's MHRA claim must be dismissed because Netgain did not "release" any health records. (Def.'s Mem at 39–43.) The Court agrees.

Minnesota law provides as follows:

> A person who does any of the following may be liable to a patient for compensatory damages caused by an unauthorized release or an intentional, unauthorized access, plus costs and reasonable attorney fees:
>
> (1) negligently or intentionally requests or releases a health record in violation of sections 144.291 to 144.297 . . . .

Minn. Stat. § 144.298, subd. 2. The Minnesota Supreme Court explained that "a person must *affirmatively* release a record that was not authorized for release by the patient's consent." *Larson v. Nw. Mut. Life Ins. Co.*, 855 N.W.2d 293, 302 (Minn. 2014) (emphasis added). And the court defined "release" to mean "[t]o set free from . . . [or] let go" or "[t]o make available for use." *Id.* (alterations in original).

Applied here, Netgain never affirmatively released the health records to the cybercriminals. Instead, as is alleged in the Amended Complaint, the cybercriminals exfiltrated (i.e., stole) Plaintiffs' Sensitive Information. (Am. Compl. ¶¶ 6, 41.) And a stealing does not constitute an affirmative release as required by the statute.[6]

d. Declaratory Judgment

Netgain contends that Plaintiffs' request for a declaratory judgment fails because it seeks "nothing more than a ruling on Plaintiffs' other claims." (Def.'s Mem. at 44.) Further, Netgain contends that Plaintiffs' request for relief should be dismissed because they only seek injunctive relief, which it contends is not available here because Plaintiffs have other adequate legal remedies and because there is no ongoing, irreparable injury to enjoin. (*See id.* at 44–45.)

---

[6] Because the Court dismisses the MHRA claim on this basis, the Court need not consider Defendant's alternative arguments. (*See* Def.'s Mem. at 40, 43.)

The Declaratory Judgment Act permits the judiciary to "declare the rights and other legal relations of any interested party seeking such declaration, whether or not further relief is or could be sought." 28 U.S.C. § 2201(a). To proceed successfully under the Declaratory Judgment Act, there must be a "substantial controversy" that presents a "concrete and specific" question. *Caldwell v. Gurley Refining Co.*, 755 F.2d 645, 649–50 (8th Cir. 1985) (internal quotation marks and citation omitted).

Netgain's arguments are premature at this stage of the litigation. Plaintiffs allege that Netgain continues to provide "inadequate and unreasonable" data security, and that they and the Class "continue to suffer injury." (Am. Compl. ¶ 151.) This is enough to survive a motion to dismiss. *See In re Arby's Rest. Grp. Inc. Litig.*, No. 1:17-cv-0514-AT, 2018 WL 2128441, at *15 (N.D. Ga. Mar. 5, 2018) (denying motion to dismiss the declaratory judgment claim); *In re: The Home Depot, Inc., Customer Data Sec. Breach Litig.*, No. 1:14-MD-2583-TWT, 2016 WL 2897520, at *4–5 (N.D. Ga. May 18, 2016) (denying motion to dismiss claims for declaratory and injunctive relief).

III. CONCLUSION

Based on the submissions and the entire file and proceedings herein, **IT IS HEREBY ORDERED** that Defendant Netgain Technology, LLC's Motion to Dismiss [Doc. No. 45] is granted in part and denied in part, as follows:

1. The Motion is **GRANTED** as to Counts II and V;
2. The Motion is **DENIED** as to Counts I and VI; and
3. The Motion is **DENIED** as moot as to Counts III and IV.

Dated: June 2, 2022

s/Susan Richard Nelson
SUSAN RICHARD NELSON
United States District Judge